NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

REGULATING NATION-STATE CYBER ATTACKS IN COUNTERTERRORISM OPERATIONS

by

Colleen E. Garcia

June 2010

Thesis Co-Advisors: Dorothy Denning
James Russell

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Regulating Nation-State Cyber Attacks in Counterterrorism Operations		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Colleen E. Garcia			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** **A**	

13. ABSTRACT

In August 2008, a military conflict between Georgia and Russia occurred in South Ossetia and Abkhazia. Russian military action in this conflict was immediately preceded by a number of cyber attacks against a variety of Georgian Government Web sites, and while the perpetrator(s) was never conclusively identified, Russia denied involvement. Importantly, however, the Georgian cyber attacks seem to be the first instance of cyber attacks used in combination with conventional attacks. In combating each other through the kinetic attacks used to date, nation-states have been required to comply with the long-standing law of armed conflict. Yet, modern warfare now challenges this accepted regulation in two ways. First, as was just demonstrated, cyber attacks now may complement traditional kinetic attacks. And second, it is not fellow states that nations now commonly face in combat as people suspected was the case during the Georgian attacks, but rather nonstate actors, a fact made evident by the ongoing Global War on Terror. This thesis will therefore seek to answer two questions: (1) Are existing international laws governing cyber attacks conducted by nation-states against terrorists sufficient? (2) If existing law is insufficient, how should international law be amended to better regulate the use of such cyber attacks in counterterrorism operations? To test the idea of sufficiency, the thesis will first examine potential nation-state cyber-attack scenarios that may be seen in future counterterrorism operations, and whether those possible attack scenarios are in keeping with international law principles. This assessment ultimately demonstrates that problems of evaluation and enforcement stymie attempts at regulation of nation-state cyber attacks in counterterrorism operations, creating new areas of concern for international law, which can only be resolved through the creation of cyber attack-specific legal principles and enhanced enforcement mechanisms.

14. SUBJECT TERMS: Cyber attack, International Law, China, Russia, United States, al Qaeda, Hamas, Hezbollah, FARC, Botnet, Worm, Virus, Malicious Code, Hack, *jus in bello, jus ad bellum*, Law of Armed Conflict (LOAC), Laws of War, Counterterrorism Operations (CT), Cyber Strategy, Military Strategy, Foreign Policy, National Policy, Use of Force, Armed Attack, Enforcement, Evaluation			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

REGULATING NATION-STATE CYBER ATTACKS IN COUNTERTERRORISM OPERATIONS

Colleen Elizabeth Garcia
Department of Defense Civilian
B.S.F.S., Georgetown University Edmund A. Walsh School of Foreign Service, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(COMBATING TERRORISM: POLICY AND STRATEGY)

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Author: Colleen E. Garcia

Approved by: Dorothy E. Denning
Thesis Co-Advisor

James A. Russell
Thesis Co-Advisor

Harold Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In August 2008, a military conflict between Georgia and Russia occurred in South Ossetia and Abkhazia. Russian military action in this conflict was immediately preceded by a number of cyber attacks against a variety of Georgian Government Web sites, and while the perpetrator(s) was never conclusively identified, Russia denied involvement. Importantly, however, the Georgian cyber attacks seem to be the first instance of cyber attacks used in combination with conventional attacks. In combating each other through the kinetic attacks used to date, nation-states have been required to comply with the long-standing law of armed conflict. Yet, modern warfare now challenges this accepted regulation in two ways. First, as was just demonstrated, cyber attacks now may complement traditional kinetic attacks. And second, it is not fellow states that nations now commonly face in combat as people suspected was the case during the Georgian attacks, but rather nonstate actors, a fact made evident by the ongoing Global War on Terror. This thesis will therefore seek to answer two questions: (1) Are existing international laws governing cyber attacks conducted by nation-states against terrorists sufficient? (2) If existing law is insufficient, how should international law be amended to better regulate the use of such cyber attacks in counterterrorism operations? To test the idea of sufficiency, the thesis will first examine potential nation-state cyber-attack scenarios that may be seen in future counterterrorism operations, and whether those possible attack scenarios are in keeping with international law principles. This assessment ultimately demonstrates that problems of evaluation and enforcement stymie attempts at regulation of nation-state cyber attacks in counterterrorism operations, creating new areas of concern for international law, which can only be resolved through the creation of cyber attack-specific legal principles and enhanced enforcement mechanisms.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AFCYBER	United States Air Force Cyber Command
ATS	Atlantic Treaty System
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CNS	Center for Nonproliferation Studies
CYBERCOM	Cyber Command
DoD	United States Department of Defense
DOS	Denial of Service
FARC	Revolutionary Armed Forces of Columbia
IAEA	International Atomic Energy Agency
ICAR	International Centre for Asset Recovery
ICC	International Criminal Court
ICJ	United Nations International Court of Justice
IDS	Intrusion Detection System
ISP	Internet Service Provider
LLTE	Liberation Tigers of Tamil Eelam
LOAC	Law of Armed Conflict
NSF	National Science Foundation
RIRA	Real Irish Republican Army
UN	United Nations
USSTRATCOM	United States Strategic Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to thank, first and foremost, her thesis advisors: Professor Dorothy Denning for inspiring her interest in the subject, and for patiently and painstakingly increasing her knowledge of it; and Professor James Russell for his unwavering personal support and commitment to the final product.

She would also like to acknowledge the constant encouragement of her family and friends throughout the writing and approval processes. Their backing proved critical to the completion of this work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. INTRODUCTION

In August 2008, a military conflict involving land, air, and sea forces of Georgia and Russia occurred in South Ossetia and Abkhazia, provinces under the nominal control of Georgia. Russian military action in this conflict was immediately preceded by a number of cyber attacks against a variety of Web sites of the Georgian government. The perpetrator(s) was never identified, and Russia denied involvement. The National Research Council notes, "The primary significance of the cyber attacks on Georgia is that they appear to be the first instance of simultaneous actions involving cyber attack and kinetic attack."[1] Cyber technology had officially entered into modern warfare.

Evidence now clearly shows that nations have already long been developing cyber technology as another weapon of attack. John A. Serbian, Jr., Information Operations Issue Manager at the CIA, reports that:

> We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs…They are developing strategies and tools to conduct information attacks.[2]

According to Peter Brookes, a Senior Fellow for National Security Affairs at the Heritage Foundation, "more than 100 countries are developing the ability to use the Web for spying or as a weapon, including China, Russia, Iran, and North Korea."[3] The Georgian cyber attacks, however, stunned nations across the globe into realizing that cyber capability had been met with a willingness to wield it in war.

---

[1] William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or CyberAttack Capabilities* (Washington, DC: The National Academies Press, 2009), 3–21.

[2] John A. Serabian, "Cyber Threats and the U.S. Economy," Central Intelligence Agency, https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html.

[3] Peter Brookes, "The Cyberspy Threat: Foreign Hackers Target Military," Family Security Matters, http://www.familysecuritymatters.org/publications/id.3103/pub_detail.asp.

In combating each other through the kinetic attacks, nation-states have been required to comply with the long-standing law of armed conflict (LOAC). Modern warfare now challenges this accepted regulation in two ways; (1) Cyber attacks now may complement traditional kinetic attacks and; (2) It is unclear whether that regulatory framework is appropriate to govern adversarial interactions between state- and non-state actors.

As conflict between developed states dramatically declined after World War II, developed states, in particular, entered into armed conflict with guerilla groups and what many would characterize today as terrorist organizations.[4] During the second half of the twentieth century, nation-states became increasingly engaged in conflict against violent non-state actors seeking to use terrorist tactics to achieve their political objectives. This was the case, for example, during Great Britain's extended bloody struggle against the Irish Republican Army, and it is the case for America's current Global War on Terror. Militaries from developed states around the world now routinely conduct counterterrorism operations against violent non-state actors.

Given these challenges presented by cyber technology and state-versus-nonstate conflict, how well then do the established laws of war hold up against nation-state cyber attacks in counterterrorism operations?

B. BACKGROUND AND SCOPE

As previously noted, the rules of state-to-state combat are clear and well respected. *Jus ad bellum* codified by the United Nations Charter outlines when nations may use force, and *jus in bello* arising from the Hague Conferences, the Geneva Conventions and customary international law specifies how that force may be applied during war. The application of these legal principles and regulations to nation-state battles with no state actors has proved slightly more obscure. Nonstate actors are not addressed by international law, a fact made glaringly obvious by current counterterrorism legislation.

[4] Daniel Moran, *Wars of National Liberation* (New York: Harper, 2006).

Creating and amending international law is an intentionally slow process, out of deference for the gravity of its application, and out of respect for the protection of sovereignty. Yet nations have been consistently facing terrorists since the end of World War II, and only piecemeal legislative conventions exist, all of which have little to no guidance for military counterterrorism operations. This issue is vital to address, given the commonality of this type of conflict.

On the other hand, there has been a great deal of literature written regarding the relevance of existing international law to nation-state cyber attacks. Scholars largely agree that portions of the law of armed conflict, international humanitarian law, and international human rights law are applicable, and indeed binding, upon a nation-state's use of cyber attacks. What is less well known is whether these bodies of international law are sufficient to regulate these attacks, particularly on the dubiously governed battlefield of counterterrorism operations.

There is also a question of enforcement. It is critical to distinguish insufficiency of international law itself versus insufficiency of its enforcement. If there is an inadequacy in either, answering this question is essential to determining how international law, or its enforcement, can best evolve to govern nation-state cyber attacks in counterterrorism operations.

This thesis seeks to answer two questions: (1) Are existing international laws governing cyber attacks conducted by nation-states against terrorists sufficient? (2) If existing law is insufficient, how should conventional and customary international law be amended to better regulate the use of such cyber attacks in counterterrorism operations?

C. METHODOLOGY

To answer these questions, this thesis will study the existing conventional and customary international laws governing nation-state cyber attacks against terrorists, as well as the current status of such attacks. It will examine the application of international laws to potential nation-state cyber attacks that may occur against terrorist groups, given the current cyber capability of nation-states as well as the cyber technology use by terrorists. It will then decide whether international laws are sufficient to regulate attacks

that violate existing law. In order to test the idea of sufficiency, the thesis will first examine potential nation-state cyber-attack scenarios that may be seen in future counterterrorism operations, and whether those possible attack scenarios are in keeping with international law principles. This examination of possible attacks scenarios will decide the level of international cyber law sufficiency, as well as the necessary legal evolution.

D. OVERVIEW

Chapter I introduced the main research question: Are international laws governing nation-state cyber attacks against nonstate actors sufficient? It then posed the follow-up question: If insufficient, how should international laws governing these attacks be amended?

Chapter II will establish the importance of answering these questions. It will first define the term "cyber attack," and then examine the broad history of nation-states as cyber attackers, focusing on the perceived threat, the present reality, and possible futures. It will also lay out the extensive use of cyber technology by terrorists. This will lay the groundwork for introducing terrorist networks as targets of nation-state cyber attacks. This chapter will argue that, given the likely use of cyber attacks in military settings, and also given that nations are increasingly countering terrorists in this military context, there is a high probability that nation-states *will* use cyber attacks against terrorists in the future, if they are not already.

Chapter III will begin by looking at legislation relevant to counterterrorism operations. It will examine the general status of international law governing terrorism. It will highlight what is already a grossly inadequately governed battlefield. It will then follow by offering a broad discussion of existing customary and conventional international law regulating nation-state cyber attacks. It will note the relevant principles of the law of war, humanitarian law, and human rights law that apply. The chapter will conclude that current international laws apply to these attacks, and then it will examine whether these same international laws are sufficient to govern them.

Chapter IV will lay out potential nation-state cyber attack scenarios that may be seen in future counterterrorism operations. With each scenario, this chapter will examine its legality under the international law of armed conflict. It will then look more broadly at holes in existing customary and conventional international law presented by each of the scenarios.

Finally, Chapter V will conclude the thesis by proposing solutions on how to address the gaps presented in Chapter IV with current and future international law efforts. It will first examine problems of evaluation, and how this hamstrings international regulation. This chapter will then also take up the question of enforcement. This is a long-standing issue with international law, and efforts to regulate cyber attacks are no different.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CAPABILITY DEVELOPMENT MEETS ATTACK WILLINGNESS

As previously mentioned, many states are actively developing cyber capabilities for military use in war. As terrorist groups increasingly use cyber technology to further their goals, they leave themselves open to nation-state cyber attacks. It is only a matter of time before this vulnerability is exploited by nation-states in their counterterrorism operations. International law must evolve to address that behavior, as it has done so often to regulate innovative military weapons of the past.[5]

A. TERRORISTS AND CYBER TECHNOLOGY

States have historically been willing and eager to employ improved weapons on the battlefield to beat their adversaries, and cyber technology may prove no different. Terrorists have increased their use of cyber technology to gain advantages, but this has also left them vulnerable to the skillful cyber attacks of technologically advanced nations. The National Research Council recounts, "Although the weapons of terrorists are generally low-tech, their use of the Internet and information technology for recruitment, training, and communications is often highly sophisticated."[6] Terrorist groups are increasingly using this sophistication to advance their goals. There have been examples of this worldwide, as the necessary technology has spread. Terrorist groups are using cyber technology to enhance their already effective traditional methods.

Daniel Byman notes, "terrorists use the Internet for its commonly accepted benefits: communication, propaganda, marketing, and fundraising."[7] Gabriel Weimann has identified seven different instrumental uses of the Internet for terrorism: data mining; networking the terrorists; recruitment and mobilization; instructions and online manuals;

---

[5] Andreas Laursen, *Changing International Law To Meet New Challenges: Interpretation, Modification And The Use of Force* (Portland: Djoef Publishing, 2006).

[6] William A. Owens, Kenneth W. Dam and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities* (Washington, DC: The National Academies Press, 2009), 9.

[7] Daniel Byman, *The Five Front War: The Better Way to Fight Global Jihad* (Hoboken, NJ: John Wiley & Sons, Inc., 2008), 50.

planning and coordination; fund-raising; and attacking other terrorists.[8] He finds that "the great virtues of the Internet have been converted to the advantage of groups committed to terrorizing societies in order to achieve their goals."[9]

Furthermore, cyber activity is not just limited to one terrorist network. Rather, various terrorist networks across the globe are active in cyberspace, though they fall largely into two different groups: non-Islamic and Islamic terrorists, both of which target potential sympathizers, the international community, and their adversaries.

1. Non-Islamic Terrorists

The Liberation Tigers of Tamil Eelam are one non-Islamic terrorist group that has used cyber technology extensively. Shyam Tekwani details:

> The LLTE was quick to grab the opportunity to tell its own side of the story with the emergence of the Internet. The Internet has emerged as the single most important weapon in the arsenal of Tamil militants and is an important means for the Tamil diasporas to keep abreast of events in the homeland.[10]

The Internet Black Tigers, an offshoot of the Tamil Tigers, has also conducted cyber attacks. Professor Dorothy Denning reports:

> In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read 'We are the Internet Black Tigers and we're doing this to disrupt your communications.' Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.[11]

Though their physical attacks are well known, the Real Irish Republican Army (RIRA) is another terrorist group that has been active in cyberspace. Weimann notes that, in addition to its recent 2009 army base attack and 2010 car bomb, RIRA's Web site

---

8 Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 111–145.

9 Ibid., 29.

10 Shyam Tekwani, "The Web of Terror," *Media* Asia 29, no. 3 (2002): 146–149.

11 Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives," Georgetown University, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

use ranges from fundraising to preparing a possible attack on Prince William, causing many of their sites to be shutdown due to their perceived threat to security.[12] Such sites are prime targets for nation-state cyber attacks.

Aum Shinrikyo in Japan has also been an interesting case of terror on the Internet in the past. Weimann demonstrates that they utilized cyber activity to paint a particular image of being an organization interested solely in spiritual well being, despite their well-publicized chemical weapons attack on the Japanese subway in 2005.[13] Aum Shinrikyo now employs the Internet to persuade others of their movement back to their spiritual underpinnings.

Finally, perhaps one of the most impressive terrorist uses of cyber technology is that of the Revolutionary Armed Forces of Colombia (FARC). On their activity, Weimann states, "The sophisticated Web sites of FARC…are an impressive example of media-savvy Internet use by a terrorist group…The FARC Web sites are more 'transparent,' stable, and mainly focused on information and publicity."[14] FARC Web sites can be found in multiple languages, and they cover a variety of subjects. They speak to everything from Columbia's domestic and international policy, the country's socioeconomic issues, to U.S. activity at home and abroad.

2. Islamic Fundamentalist Groups

The greatest current amount of cyber activity, however, appears to come from a seemingly unlikely group: Islamic fundamentalist terrorist organizations. On Islamic fundamentalism and cyber technology, Weimann says, "Many of the terrorists on the Net belong to radical Islamist groups and organizations. Paradoxically, it is those who criticize and attack Western modernity, technology, and media who are using the West's most advanced modern medium, the Internet."[15] These Islamic fundamentalist groups

---

[12] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C.: United States Institute of Peace Press, 2006), 92–96.

[13] Ibid., 59–61.

[14] Ibid., 75.

[15] Ibid., 51.

utilize cyber technology to further their jihadist aims. In what is sometimes called, "electronic jihad," "jihadist forums are used to distribute manuals and tools for hacking, and to promote cyber attacks," which sometimes "coincides with physical forms of terrorism and protest."[16] Al Qaeda and those associated with it have been known to utilize electronic jihad, and is one of the most active terrorist groups, if not the most active terrorist group, on the Web.

Daniel Byman explains, "Al-Qa'ida professes a peculiar mixture of ancient ideology fused to cutting-edge technology. More than any other terrorist group in history, it has seized on the communications revolution systematically and creatively."[17] He continues to say that booming jihadist Web sites include "various official or semiofficial statements from the al-Qa'ida leadership. They make available documents important to the jihad—such as manuals outlining various fighting techniques—and testimonies from martyrs who died fighting American, Russian, or other foreign troops."[18] These technologically advanced Web sites are, by and large, user friendly and can be accessed in multiple languages:

> These sites serve several purposes. Perhaps most important, they spread the ideas that al-Qa'ida champions: the need for jihad, the corruption of Muslim governments, and the evil of the United States. Proselytization follows, with appeals for recruiting men and raising money.[19]

For all these reasons, al Qaeda has come to rely heavily on cyber technology.

Expert Paul Eedle notes:

> The Web site is central to al Qaeda's strategy to ensure that its war with the U.S. will continue even if many of its cells across the world are broken up and its current leaders are killed or captured. The site's function is to deepen and broaden worldwide Muslim support, allowing al Qaeda or successor organizations to fish for recruits, money and political backing.

---

[16] Dorothy E. Denning, "Terror's Web: How the Internet Is Transforming Terrorism," in *Handbook on Internet Crime*, eds. Yvonne Jewkes and Majid Yar (Portland: William Publishing, 2009).

[17] Daniel Byman, *The Five Front War: The Better Way to Fight Global Jihad* (Hoboken, NJ: John Wiley & Sons, Inc., 2008), 177.

[18] Ibid.

[19] Ibid.

> The whole thrust of the site, from videos glorifying September 11 to Islamic legal arguments justifying the killing of civilians, and even poetry, is to convince radical Muslims that, for decades, the U.S. has been waging a war to destroy Islam, and that they must fight back.[20]

Such vast Web activity makes al-Qaeda prime targets for cyber attacks, attacks that would be easy to implement even now as part of the Global War on Terror.

Hezbollah is another major Islamic group that engages in cyber activity. Weimann argues that this terrorist group:

> …opposes the West, seeks to create a Muslim fundamentalist state modeled on Iran and to liberate Jerusalem and ultimately eliminate Israel, and has advocated the ultimate establishment of Islamic rule in Lebanon… [Hezbollah] was one of the first terrorist organizations to establish and operate a large network of linked Web sites in several languages.[21]

He describes their cyber activity noting:

> The official Web site of Hezbollah is the Central Press Office. This is an impressively designed, advanced, regularly updated site in English and Arabic. It presents political declarations, public statements, transcripts of speeches given by Sheikh Nasrallah, photos, songs celebrating jihad, and a collection of videotapes to be viewed or downloaded.[22]

This is not the only site, however. "Hezbollah also operates the al-Manar Web site…The al-Manar Web site offers video broadcasts of the television station as well as transcripts from the station's English news."[23] Such an impressive array of cyber activity makes Hezbollah an attractive target for nation-state cyber attacks.

Hamas has also become more involved with furthering terrorism on the Internet. The Internet is very popular among children and youth. Terrorists know this and are using the Internet increasingly to target children for recruitment. Weimann warns, "One

---

[20] Paul Eedle, "Terrorism.com," *Guardian*, July 17, 2002, http://www.guardian.co.uk/print/0,3858,4462872-103680,00.html.

[21] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 88.

[22] Ibid., 89.

[23] Weimann, *Terror on the Internet*, 88.

of Hamas' Web sites…is updated every other week and is designed for children, with a cartoon-style design and colorful children's stories."[24] This targeting of children is concerning as it starts them on the terrorist path early, making them more difficult to counter later after years of radicalization.

Terrorists, therefore, have demonstrated an increasingly widespread use of cyber technology. As is always the case with use of cyber technology, terrorists face both the advantage of advancement, and the possible disadvantage of attack. Such a disadvantage is in fact, likely, given that the large majority of cyber attacks will cause much less, if any collateral damage, then conventional kinetic attacks. When conducting such cyber attacks, it is critical that nations either play by the rules, or that rules are created for them.

B. WHAT IS A CYBER ATTACK?

In order for international law to regulate cyber attacks, it is critical to be able to first recognize them. For that reason, defining "cyber attack" is essential. The National Research Council defines the term as:

> *Cyber attack* refers to the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Such effects on adversary systems may also have indirect effects on entities coupled to or reliant on them. A cyber attack seeks to cause adversary computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary.[25]

The United States Department of Defense has its own definition, which is particularly relevant to nation-state cyber attacks. It considers computer network attack

[24] Weimann, *Terror on the Internet*, 91–92.

[25] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities*, (Washington, DC: The National Academies Press, 2009), 10–11.

(CNA) to be "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[26]

Such cyber attacks are an attractive military option for nation-states for several reasons. First, there will likely be a great deal less collateral damage. Furthermore, nations can target larger portions of a big, decentralized terrorist network through cyberspace, than they can through physical space. In addition, cyber technology is a superior weapon for technologically advanced nations, giving them an edge in combat that they may employ using various techniques.

Given the many different kinds of cyber attack methods, the United States Government is particularly concerned with potential cyber attacks launched through Botnets, or Bot Networks. Scholar Clay Wilson defines Botnets as:

> …vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds of thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code.[27]

Attackers are able to do this by turning infected computers into "zombies," subject to their command. Wilson continues to report that the newest trends in Botnet crimes include: malicious code (including viruses) hosted on Web sites, identity theft, and cyber espionage, among others.[28] In explaining their startling success, Wilson describes:

> Networked computers with exposed vulnerabilities may be disrupted or taken over by a hacker, or by automated malicious code. Botnets opportunistically scan the Internet to find and infect computer systems…Compromised computers are taken over to become slaves in a "botnet," which can include thousands of compromised computers that are

---

[26] Cyberspace and Information Operations Study Center, "Computer Network Operations & Network Warfare Operations," Air University, http://www.au.af.mil/info-ops/netops.htm.

[27] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" (Washington, DC: Congressional Research Service, 2008), 5.

[28] Wilson, "Botnets, Cybercrime, and Cyberterrorism," 10–12.

> remotely controlled to collect sensitive information from each victim's PC, or to collectively attack as a swarm against other targeted computers.[29]

It is likely that nation-states themselves would choose to use one, or a combination of other more practical, cyber attack technologies against terrorists, including: rootkits, exploits, sniffers, phishing, malware, spyware, keyloggers, identity theft, smurfing, DOS attacks, spoofing, routing attacks, cyber-herding, Web defacement, and legitimate shutdown.

Rootkits are often used in conjunction with system penetrations. Edward Skoudis defines rootkits as "software that alters the operating system to lie about and hide the attacker's files, programs, and network communications, thus concealing the attacker's presence on a machine."[30] The attacker here would be a nation-state employing malware to gain systemic control of terrorists' computers without detection.

Exploit code is form of malware that exploits vulnerabilities in software in order to gain access to a system. Skoudis describes using exploit code to take advantage of software's inherent vulnerabilities, saying, "The software at the heart of major infrastructure devices may have bugs or flaws; most are mere annoyances, but attackers might deliberately trigger some flaws to harm a system."[31] Nations can use such software bugs against terrorist computers, though more likely on a smaller scale.

"Sniffing" provides a way to monitor the Web activity of jihadists. Gabriel Weimann explains:

> Capturing traffic over the Net is called 'sniffing,' with 'sniffer' being the software that searches the traffic and grabs those items it is programmed to find. Intrusion detection systems (IDSs) use sniffers to match transmitted data, including e-mail messages, against a set of rules.[32]

---

29 Wilson, "Botnets, Cybercrime, and Cyberterrorism," 24.

30 Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defesnse University, 2009), 175.

31 Ibid., 182.

32 Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 183.

Carnivore is an example of a sniffing program used for domestic monitoring, though such technology can be used against terrorists as well.

Phishing attacks are commonly used against nation-states, but they can be used by them as well. Skoudis writes that phishing attacks typically involve emails from a seemingly legitimate company trying to:

> …dupe users into clicking on a link that appears to point to a legitimate business Web site but actually takes the user to an imposter site controlled by the attacker and designed to resemble the e-commerce site. The site asks for a login name and password or other account information, which the attacker's software retains for fraud and criminal use.[33]

Instead of criminal use, nations could employ phishing attacks against terrorists for the purposes of surreptitious monitoring.

Nations can also utilize the same types of malware, or malicious code, so often employed by nonstate actors: Trojan Horses, viruses, and worms. In explaining the difference between these types of malware, the National Research Council documents:

> Worms and viruses are techniques generally used for installing Trojan horses on many computers. A worm is self-replicating—in addition to infecting the machine on which it is resident, it uses that machine to seek out other machines to infect. A virus replicates through actions—for example, an email.[34]

All these forms of malware can be used to infect terrorist computers in many different ways, with the ultimate goal ranging from data exfiltration, to systemic damage, and even to total destruction.

Nations may also take advantage of different forms of spyware in their various counterterrorism operations. Skoudis states that spyware "focuses on gathering information from and about users and is installed on a user's machine without notice or

---

[33] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyber power and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University, 2009), 175.

[34] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber Attack Capabilities* (Washington, DC: The National Academies Press, 2009), 97.

consent."[35] One of the most common ways to do this is though a keylogger. "Keyloggers are small programs invisibly installed on a computer that record all keyboard input. An attacker can use this to (e.g.) record passwords."[36] Once this password information is extracted from terrorists, it can be used to log in to secure emails, chat rooms, and Web forums.

Identity theft is one of the most common cyber crimes committed against innocent civilians, but it can also be used against terrorists. Nation-states can impersonate high-level terrorist group leaders, for example, thereby confusing and misleading their unsuspecting followers.

Denial-of-service (DOS) attacks can also be of great use to governments. The National Research Council writes that each DOS attack "floods a specific target with bogus requests for service, thereby exhausting the resources available to the target to handle legitimate requests for service and thus blocking others from using those resources."[37] Nation-states could utilize DOS attacks, with the ultimate goal being decreased availability and functionality of terrorists' Web activity.

Nations can then also conduct spoofing attacks against terrorists, with the intention of sowing deception. On this, Weimann and Von Knop note, "A spoofing attack occurs when one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage."[38] It can be used to intentionally confuse identities for the purposes of misinformation amongst terrorists.

---

[35] Edward Skoudis, "Information Security Issues in Cyberspace," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defesnse University, 2009), 172.

[36] Emsisoft, "Dictionary of Computer Security Terms," Emsisoft, http://www.emsisoft.com/en/kb/articles/tec080424/.

[37] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities*, (Washington, DC: The National Academies Press, 2009), 95.

[38] Gabriel Weimann and Katharina Von Knop, "Applying the Notion of Noise to Countering Online Terrorism," *Studies in Conflict & Terrorism* 31:1(2008), 893.

Nations can also employ routing attacks against terrorist Web sites. According to Weimann and Von Knop, "The end result of any routing attack is the redirection of traffic on the network."[39] Governments can redirect traffic to pass through their own network, and thereby monitor the traffic. By taking control of online traffic, nation-states can assume power not just over the communication between two or more entities, but also over their larger networks. This could be particularly useful against large, decentralized terrorist networks whose actions and connectivity may be difficult to monitor physically.

Cyber-herding is the specific counterterrorism tool advocated by David B. Moon. He writes, "Cyber-herding is the action by which an individual, group, or organization drives individuals, groups, or organizations to a desired location within the electronic realm."[40] In this case, cyber-herding can be used to imperceptibly direct Islamic fundamentalists from terrorist Web sites to secretly controlled government Web sites. Attackers are able to covertly disable the true terrorist Web activity by creating a realistic doppelganger of identified sites and chat rooms, along with corresponding private virtual networks, to attract terrorists away from the true terrorist Web activity, and then destroy that activity. In the mean time, this would allow continued intelligence on terrorists' Web activity, without alerting the terrorists of the need to re-establish or relocate their Web sites.

Another attack technique is Web defacement. According to Dr. Yona Hollander:

> Web defacement occurs when an intruder maliciously alters a Web page by inserting or substituting provocative and frequently offending data. The defacement of an organization's Web site exposes visitors to misleading information until the unauthorized change is discovered and corrected.[41]

Nation-states can employ this technique against numerous terrorist Web sites currently in existence.

---

[39] Gabriel Weimann and Katharina Von Knop, "Applying the Notion of Noise to Countering Online Terrorism," *Studies in Conflict & Terrorism* 31:1(2008), 894.

[40] David B. Moon, "Cyber-Herding: Exploiting Islamic Extremists Use of the Internet" (Monterey, CA: Naval Postgraduate School, 1997).

[41] Yona Hollander, "Prevent Web Site Defacement," Internet Security, http://www.mcafee.com/us/local_content/white_papers/wp_2000hollanderdefacement.pdf.

Though it is not an attack, a final strategy nations may use in counterterrorism operations is forcing a legitimate shutdown. This is most easily done domestically, within established laws. A nation can also appeal to another country to request that it force the shutdown of terrorist Web sites run within its territorial boundaries.

Many cyber attack methods have been presented here, and will be examined again in a later study of specific attack scenarios. Such numerous technique options demonstrate the expansive cyber capability currently at the hands of nation-states. The choice of attack technique, or combination of techniques, will ultimately depend on a nation's preference, given its end goal. All attack techniques must ultimately remain in keeping with international law.

C. THE NATION-STATE CYBER ATTACKER

As indicated earlier, nations across the globe have been working to improve their cyber capabilities. Yet this capability is also joined by a willingness to act. Nation-state intelligence has now come to present a formidable cyber threat. Peter Brookes reports, "In recent years, the threat has grown from probes by amateur hackers to premeditated, government-sponsored assaults for the purposes of penetrating or affecting political, military, economic and industrial information or operations."[42] As *Washington Times* contributor, Bill Gertz, warns, the United States is now entering an international cyber arms race, where "China, the United States, and Russia are matched equally in the new type of warfare."[43] These nations, and others, may choose to use this technology against each other, as well as against nonstate actors.

China has demonstrated a desire to pursue cyber attack technology for military purposes. The greatest number of cyber attacks arises from within Chinese national borders. The government's role is unclear, but Gertz reports that the nation "runs a national competition for college and grad school students who may currently be hacking

---

42 Peter Brookes, "The Cyberspy Threat: Foreign Hackers Target Military," Family Security Matters, http://www.familysecuritymatters.org/publications/id.3103/pub_detail.asp.

43 Bill Gertz, "China blocks U.S. from Cyber Warfare," *The Washington Times*, http://washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/.

illegally, but who could be effectively employed in creating and using new attack techniques."[44] Such skills have already been used to target the United States. Alan Paller writes, "Testimony before the House Homeland Security Committee in April 2007 revealed that both State Department and Commerce Department computers had been penetrated, most probably by government-funded actors in China."[45] If China is already targeting other nations, it is likely they will use the same cyber technology against terrorists as well. "The Chinese are going after military technology, and it's not always obvious what they've got, and what they haven't. This increases the probability of some nasty, and painful, surprises when the shooting starts."[46]

Russia is also a key cyber player on the international scene. Susan Collins reports, "Intelligence officials have stated that China and Russia have [both] attempted to map the United States' electrical grid and have left behind software that could be activated later, perhaps to disrupt or destroy components."[47] Furthermore, serious accusations have been made about Russian cyber attacks against other nations, including the previously mentioned attacks preceding and during its military confrontation with Georgia. This brings up the possibility of similar cyber attacks on terrorists before counterterrorism operations.

Even the United States has expressed intentions to utilize cyber technology in combat. The National Research Council finds it possible to imagine that:

---

44 Bill Gertz, "China blocks U.S. from Cyber Warfare," *The Washington Times*, http://washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/

45 Alan Paller, Paper presented to the United States Senate Committee on Homeland Security and Government Affairs, Washington, D.C., April 28, 2009.

46 Strategy World, "More Scary Monsters," *Strategy World*, http://www.strategypage.com/htmw/htiw/articles/20090423.aspx.

47 Susan M. Collins, Paper presented to the United States Senate Committee on Homeland Security and Government Affairs, Washington, DC, April 28, 2009.

> …cyber attack would naturally be part of a robust U.S. military posture…For the record, the U.S. government has acknowledged that it has an interest in such capabilities as a possible instrument of national policy, but this is virtually all that it acknowledges publicly.[48]

That being said, there has been a great deal of overt government activity intended to bolster U.S. cyber capabilities. The Department of Defense has created a Cyber Command (CYBERCOM) within the United States Strategic Command (USSTRATCOM), aimed at both cyber offense and defense.[49] The United States Air Force has also created its own branch-specific cyber command, AFCYBER (P). Its mission is "to provide combat ready forces trained and equipped to conduct sustained combat operations through electromagnetic spectrum and fully integrate these operations with air and space operations," with the ultimate goal being to provide the United States with "sovereign options" in air, space, and cyberspace.[50]

On the nation-state cyber threat, expert James Lewis reports, "[Nations] are sophisticated, well resourced, and persistent. Their intentions are clear, and their successes are notable."[51] There is also now the sobering realization that cyber aggression has quickly become a fundamental component of national policy and military strategy.

As nations increasingly face terrorists in combat, it is probable that they will employ similar cyber attack strategies. The question is: How well is international law prepared for this military development?

---

48 William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities* (Washington, DC: The National Academies Press, 2009), 10.

49 Jordan Reimer, "U.S. Cyber Command Preparations Under Way, General Says," United States Strategic Command, http://www.stratcom.mil/news/article/150/u.s._cyber_command_preparations_under_way_general_says.

50 United States Air Force, Air Force Cyber Command Strategic Vision," Defense Technical Information Center, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060&Location=U2&doc=GetTRDoc.pdf.

51 James A. Lewis, "Securing Cyberspace for the 44th Presidency" (Washington, DC: Center for Strategic and International Studies, 2008), 13.

III. THE CURRENT STATUS OF INTERNATIONAL LAW

International laws have developed to govern conventional warfare. The emergence of information operations, with its new use of digital weapons, innovative methods of attack and distinct target range, poses a greater challenge to regulation. Some argue that cyber attacks can be regulated by drawing analogies to existing international law conventions on egregious weapons or ungoverned spaces, while others argue that the law of armed conflict (LOAC) provides the best system of governance for nation-state cyber attacks in counterterrorism operations.[52] Does either argument have merit? Is either approach enough? These questions prove difficult to answer not just because of the novelty of cyber attacks themselves, but also because of the relatively ungoverned nature of counterterrorism operations.

A. INTERNATIONAL LAW AND TERRORISM

Global terrorism has presented many challenges to regulation of the current world order. There is as yet no comprehensive international legislation to counter this threat, raising major questions regarding international law's regulation of counterterrorism operations. Anti-terrorist legislation remains piecemeal at best, stymieing efforts to counter terrorism outside of what is covered by the smaller-scale, individual conventions that follow.

1. The Law Today

As was just mentioned, until now, international law has only dealt with terrorism through a series of separate international conventions prohibiting certain terrorist acts. David Freestone writes, "The main thrust of the legal response of the international community has been the conclusion of conventions—at a regional and global level—which seek to regulate, harmonize and/or extend the claims to criminal jurisdiction of the

[52] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law* (Washington, D.C.: National Defense University, 1998); and Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375.

contracting States. In general, the conventions have been responses to particular problems."[53] To date, the specific international conventions have been:

- The 1944 Chicago Convention on International Civil Aviation
- The 1963 Tokyo Conventions on Offences Committed Onboard Aircraft
- The 1970 Hague Convention for the Unlawful Seizure of Aircraft
- The 1971 Montreal Convention for the Suppression of Unlawful Acts Against Aircraft Safety
- The 1973 United Nations Convention to Prevent and Punish Acts of Terrorism in the Form of Crimes Against Internationally Protected Persons
- The 1979 United Nations Convention Against Hostage Taking
- The 1979 European Union Convention on Physical Protection of Nuclear Materials
- The 1988 International Maritime Organization Protocol on the Suppression of Unlawful Acts of Violence at Airports
- The 1988 International Maritime Organization Convention for Maritime Safety
- The 1991 International Civil Aviation Organization Convention on the Marking of Plastic Explosives for the Purpose of Detection
- The 1997 United Nations International Convention for the Suppression of Terrorist Bombing
- The 1999 United Nations International Convention for the Suppression of the Financing of Terrorism
- The 2005 United Nations International Convention for the Suppression of Acts of Nuclear Terrorism

Of special note, is the 1998 Rome Statute, which established the International Criminal Court. This legislation currently holds the greatest significance, as it is the most comprehensive to date. Its jurisdiction over terrorism remains nascent and underdeveloped at best. Each convention, in fact, presents challenges to adequately regulating terrorism and therefore, counterterrorism operations.

53 David Freestone, "International cooperation against terrorism and the development of international law principles of jurisdiction," in *Terrorism and International Law*, ed. Rosalyn Higgins and Maurice Flory (New York: Routledge, 1997): 43.

a. The 1944 Chicago Convention on International Civil Aviation

This document established the primary rules, or freedoms, of air sovereignty. Importantly, it also established the International Civil Aviation Organization, which has since been a major player in designing international anti-terrorist legislation relevant to the skies; however, more than the skies are at stake in terrorist attacks.

b. The 1963 Tokyo Convention on Offences and Certain Other Acts Committed On Board Aircraft

According to the United Nations Office on Drugs and Crime:

> The Convention establishes a uniform approach to acts on board aircraft which are offences against penal law, or which may or do jeopardize the safety of aircraft and persons or property on board, or good order and discipline on board.[54]

This convention prohibits certain crimes on board aircraft, particularly any crime that jeopardizes the safety of the aircraft and its passengers. Once again, though terrorists have used aircraft for attacks, this convention does not address other forms of transportation safety.

c. The 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft

This convention arose out of the United Nations' realization of "a need to deter acts of 'terrorism' affecting the aviation industry," especially "an urgent need to provide appropriate measures for punishment of offenders."[55] Specifically, the contracting states agreed to both punish offenses committed on board aircraft, including

---

[54] United Nations Office on Drugs and Crime, "Convention on Offenses and Certain Other Acts Committed On Board Aircraft 1963 ('Tokyo Convention')," United Nations, http://www.unodc.org/pdf/crime/terrorism/Commonwealth_Chapter_2.pdf.

[55] Privacy International, "U.N. - Convention for the Suppression of Unlawful Seizure of Aircraft (1970)," Privacy International, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-146570.

unlawful seizure of the aircraft (hijacking), and to assist each other with criminal prosecution. Here again, only aircraft safety is addressed, the same problem that is presented by the following convention.

d. The 1971 Montreal Convention for the Suppression of Unlawful Acts Against Aircraft Safety

The Center for Nonproliferation Studies (CNS) reports that under the Montreal Convention, it is unlawful to:

> …intentionally [perform] an act of violence against a person on board a civilian aircraft in flight…[to destroy] an aircraft in service or causing damage to an aircraft that renders it incapable of flight or is likely to endanger its safety in flight; [or to place] …devices or substances likely to destroy the aircraft.[56]

This legislation also makes it a crime to be an accomplice to someone who commits these acts.

e. The 1973 United Nations Convention to Prevent and Punish Acts of Terrorism in the Form of Crimes Against Internationally Protected Persons

This U.N. Convention, like the two previous conventions, "is based on the principle of 'extradite or prosecute'"…Its central provision (Article 7):

> …requires that a person alleged to have committed certain serious attacks against diplomats and other 'internationally protected persons' should either be extradited or have his or her case submitted to the authorities for the purposes of prosecution.[57]

---

56 Inventory of International Nonproliferation Organizations and Regimes, "Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal Convention)," Center for Nonproliferation Studies, http://209.85.173.132/search?q=cache:4X_Gzst56G4J:www.nti.org/e_research/official_docs/inventory/pdfs/civair.pdf+the+1971+Montreal+Convention+for+the+Suppression+of+Unlawful+Acts+Against+Aircraft+Safety&cd=3&hl=en&ct=clnk&gl=us&client=firefox-a.

57 Audiovisual Library of International Law, "Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents," United Nations, http://untreaty.un.org/cod/avl/ha/cppcipp/cppcipp.html.

Internationally protected persons are currently understood to mean heads of state, government, foreign affair ministers, senior government officials, and diplomats. Unfortunately, this legislation only protects a small segment of the individuals likely to be targeted by terrorists.

f. The 1979 United Nations Convention Against Hostage Taking

This convention outlaws hostage taking and being an accomplice to hostage taking. A hostage taker is defined by the United Nations as:

> …[any] person who seizes or detains and threatens to kill, to injure or to continue to detain another person…in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act.[58]

This is only one terrorist act, however.

g. The 1979 European Union Convention on Physical Protection of Nuclear Materials

The European Union defines the Convention on the Physical Protection of Nuclear Material and Nuclear Facilities as "aimed at ensuring effective physical protection during the use, storage or transport of materials used for peaceful purposes, as well as preventing and fighting crime associated with this material and these facilities."[59] States party to this Convention are expected to design and implement formal procedures for the protection of nuclear materials. Yet nuclear materials will only rarely be a terrorists' weapon of choice.

---

58 Privacy International, "U.N. - International Convention Against the Taking of Hostages (1979)," Privacy International, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-146575.

59 Europa, "Activities of the European Union: Summary Legislation," http://europa.eu/scadplus/leg/en/lvb/l27080.htm.

h. The 1988 International Maritime Organization Protocol on the Suppression of Unlawful Acts of Violence at Airports

The 1988 Protocol serves as an addition to the earlier 1971 Montreal Convention for the Suppression of Unlawful Acts Against Aircraft Safety. Under this international legislation,

> …the following acts at airports serving international civil aviation are considered offenses: the unlawful and intentional use of any device, substance, or weapon against a person, against the facilities of an airport or aircraft not in service on the premises of the airport, or the disruption of the services of the airport.[60]

As with the Montreal Convention, however, airports are only one of the many environments that need protection.

i. The 1988 International Maritime Organization Convention for Maritime Safety

> The IMO Assembly directed the Maritime Safety Committee to develop, on a priority basis, detailed and practical technical measures, including both shoreside and shipboard measures, to ensure the security of passengers and crews on board ships.[61]

This resolution came in response to the increased number of maritime crimes such as piracy and armed robbery. Yet, it is not enough to regulate the seas. As was the problem with the air safety conventions, protection of only one environment leaves others vulnerable.

---

60 Inventory of International Nonproliferation Organizations and Regimes, "Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation," Center for Nonproliferation Studies, http://209.85.173.132/search?q=cache:feUTsOWRdOIJ:www.nti.org/e_research/official_docs/inventory/pdfs/airport.pdf+The+1988+Protocol+on+the+Suppression+of+Unlawful+Acts+of+Violence+at+Airports&cd=8&hl=en&ct=clnk&gl=us&client=firefox-a.

61 International Maritime Organization, "Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988," International Maritime Organization, http://www.imo.org/Conventions/mainframe.asp?topic_id=259&doc_id=686.

j. The 1991 International Civil Aviation Organization Convention on the Marking of Plastic Explosives for the Purpose of Detection

The Center for Nonproliferation Studies details that the Convention on the Making of Plastic Explosives requires state signatories:

> …to prohibit and prevent the manufacture of unmarked explosives in their territories, to prevent the movement of such explosives into or out of their territory…States Parties agree to mark plastic explosives with a chemical agent that can be detected by commercially available vapor or particle trace detectors and/or canines.[62]

The idea here is to limit the kinds of weapons available to terrorists, but this convention, too, is far from comprehensive.

k. The 1997 United Nations International Convention for the Suppression of Terrorist Bombing

Following an attack on U.S. military personnel at the Khobar Towers facility in Dhahran, Saudi Arabia, along with a wave of other international terrorist bombings:

> …the United States initiated the negotiation of the convention …[It] fills an important gap in international law by expanding the legal framework for international cooperation in the investigation, prosecution, and extradition of persons who engage in such bombings and similar attacks reports the United States House of Representatives.[63]

The Terrorist Bombing Convention was a huge step forward in terms of terrorism regulation; however, bombing is only one of many possible terrorist attacks.

---

62 Inventory of International Nonproliferation Organizations and Regimes, "Convention on the Marking of Plastic Explosives for the Purpose of Detection," Center for Nonproliferation Studies, http://209.85.173.132/search?q=cache:VKJOWWye12QJ:www.nti.org/e_research/official_docs/inventory/pdfs/pexplo.pdf+The+1991+Convention+on+the+Making+of+Plastic+Explosives&cd=2&hl=en&ct=clnk&gl=us&client=firefox-a.

63 Committee Documents, "Implementation of the International Convention for the Suppression of Terrorist Bombings and the International Convention for the Suppression of the Financing of Terrorism," United States House of Representatives, http://commdocs.house.gov/committees/judiciary/hju76122.000/hju76122_0.htm#1.

l. The 1999 United Nations International Convention for the Suppression of the Financing of Terrorism

According to the International Centre for Asset Recovery (ICAR), the 1999 Convention:

> Requires parties to take steps to prevent and counteract the financing of terrorists, whether direct or indirect, through groups claiming to have charitable, social or cultural goals or which also engage in illicit activities such as drug trafficking or gun running; Commits States to hold those who finance terrorism criminally, civilly or administratively liable for such acts; and Provides for the identification, freezing and seizure of funds allocated for terrorist activities, as well as for the sharing of the forfeited funds with other States on a case-by-case basis. Bank secrecy is no longer adequate justification for refusing to cooperate.[64]

Regulating terrorist financing addresses the root of the problem, but terrorists are also often self-financed, and still attacking.

m. The 2005 United Nations International Convention for the Suppression of Acts of Nuclear Terrorism

The National Science Foundation (NSF) states, "This convention provides for a definition of acts of nuclear terrorism and covers a broad range of possible targets, including those against nuclear power plants and nuclear reactors."[65] Following along the protocol of previous international terrorism conventions, the 2005 Convention adopted an extradite or try policy. It:

> …also encourages States to cooperate in preventing terrorist attacks by sharing information and assisting each other in connection with criminal investigations and extradition proceedings. The treaty requires that any seized nuclear or radiological material is held in accordance with the

64 Asset Recovery Knowledge Centre, "International Convention for the Suppression of the Financing of Terrorism, 1999," International Centre for Asset Recovery, http://www.assetrecovery.org/kc/node/9d9db21c-a349-11dc-bf1b-335d0754ba85.0;jsessionid=03FFFDE24A3F752DFC3E6B193031D786.

65 National Science Digital Library, "International Convention for the Suppression of Acts of Nuclear Terrorism (2005)," National Science Foundation, http://www.atomicarchive.com/Treaties/Treaty22.shtml.

> International Atomic Energy Agency (IAEA) safeguards, and handled in regard to the IAEA's health, safety and physical protection standards.[66]

As with the 1979 Convention, nuclear and radiological materials are not the only terrorist weapons of concern.

Each of these conventions presents a huge step forward for international law's regulation of terrorism. None of them addresses the threat comprehensively, which also means that none of them offers a legal, universal response for counterterrorism operations.

n. The 1998 Rome Statute and the Crime of Aggression

The closest the international community has come to a comprehensive ban on terrorism has been the 1998 Rome Statute that established the International Criminal Court (ICC). This statute gives the ICC jurisdiction over crimes of genocide, crimes against humanity, war crimes, and the crime of aggression. This last crime, the crime of aggression, could possibly include acts of terrorism. The problem is that the crime of aggression must be defined before the ICC can have jurisdiction to prosecute it, and terrorism must be defined before it can be incorporated into the defined crime of aggression. Unfortunately, there is a widespread lack of definitional consensus on both of these terms.

Regarding the crime of aggression, the Universite de Montreal has found that the three biggest issues to solve before reaching a definition have been "the question of individual criminal responsibility, the role of the U.N. Security Council, and the general scope of the definition of the crime of aggression itself."[67] It is likely that these concerns will have to be debated and solved by State parties to the Rome Statute before the ICC can acquire jurisdiction over the crime of aggression.

---

66 National Science Digital Library, "International Convention for the Suppression of Acts."

67 Papyrus: Digital Institutional Repository, "Defining the Crime of Aggression: Cutting the Gordian Knot?" Universite de Montreal, https://papyrus.bib.umontreal.ca/jspui/handle/1866/2354.

Turning to terrorism, scholar Maurice Flory notes, "there is no universally accepted definition of terrorist action in international law. Existing definitions are either limited in scope to particular facets of terrorism, or approved by only a limited number of States."[68] Many possible definitions have been offered, but no consensus definition has been accepted. Without a definition for terrorism, there can be no codification of it, limiting international law's ability to comprehensively govern counterterrorism operations.

Despite the seemingly endless number of definitions for terrorism that have been offered without agreement, there is still room for optimism. Following the horrific terrorist attacks in the United States, London, and Madrid, the United Nations came under immense pressure to confirm a definition of terrorism. Leading the charge was former U.N. Secretary-General Kofi Annan. In his report, *In Larger Freedom*, Secretary-General Annan urged the U.N. to rally behind his objective definition of terrorism:

> …any action constitutes terrorism if it is intended to cause death or serious bodily harm to civilians or non-combatants, with the purpose of intimidating a population or compelling a Government or an international organization to do or abstain from doing any act.[69]

This definition was ultimately not accepted by the United Nations. The Centre for International Governance expressed encouragement noting that "Wesley Wark, who teaches intelligence and security at the University of Toronto, said Mr. Annan's proposed definition is close to definitions in criminal legislation in a number of countries, including Canada, the United States and Britain."[70] The fact that objective definitions of terrorism already exist in the domestic legislation of such large nations sets

---

68 Maurice Flory, "International law: an instrument to combat terrorism," in *Terrorism and International Law*, ed. Rosalyn Higgins and Maurice Flory (New York: Routledge, 1997): 33.

69 United Nations, "Secretary-General Kofi Annan Launches Global Strategy Against Terrorism in Madrid," United Nations, http://www.un.org/News/Press/docs/2005/sg2095.doc.htm.

70 CIGI Online, "Annan proposes Definition of Terrorism," The Centre for International Governance Innovation, http://www.igloo.org/community.igloo?r0=community&r0_script=/scripts/announcement/view.script&r0_pathinfo=%2F{7caf3d23-023d-494b-865b-84d143de9968}%2FAnnouncements%2Fciginews%2Fannanpro&r0_output=xml.

an important precedent, and a helpful stepping-stone, to reaching a consensus definition of terrorism in international law. With the backing of such powerful international lawmakers as Secretary-General Annan, there is reason to believe that this effort to acquire a consensus definition may yet prove successful.

In spite of this recent effort to acquire definitional consensus on terrorism in international law, it is crucial to remember that this has not happened yet. Nor is it likely to occur anytime soon, if ever. Without this definitional consensus, any comprehensive international regulation of terrorism is impossible. The piecemeal conventions mentioned earlier are currently the best, and sadly, the only current method to counter terrorism in international law until an accepted objective definition of terrorism is reached. Until then, evidence suggests that nation-states will continue to combat terrorists on a battlefield on which neither belligerent is sufficiently protected from the other under international law, as is evidenced by inadequate analogies to pre-existing international conventions, and the use of age-old laws of war.

B. ANALOGIES TO EXISTING INTERNATIONAL CONVENTIONS

Turning to the novelty of cyber weapons, there are similarities in existing international conventions to draw upon for regulation of cyberspace now, and it is tempting to do so. As was demonstrated earlier, the cyber threat is a real and present concern, so making analogies to pre-existing international conventions seems a quick and easy fix for regulation. The best analogies for cyber aggression are found in today's existing nuclear warfare concerns, Space Law, the Antarctic Treaty System, International Human Rights Law, and International Humanitarian Law. Yet a brief discussion of each makes it clear that none is sufficiently applicable to the use of cyber attacks in war.

Studies show, for example, that though they would be rare, the consequences of the worst conceivable cyber attack are most comparable in extent and severity to those of nuclear warfare.[71] For this reason, many scholars and lawyers have argued that cyber

[71] Dickon Ross, "Electronic Pearl Harbor," *Guardian*, February 20, 2003.

warfare can be treated the same way as nuclear warfare.[72] This would mean that there would be no outright ban on cyber attacks, but rather that each case of cyber destruction would be evaluated individually, perhaps by the United Nations, to determine its lawfulness. Cyber attacks have been launched with greater frequency than nuclear weapons. It may not even be possible to legally address each attack in this piecemeal fashion. A broad, comprehensive piece of legislation may be more helpful.

Space law could be one such piece of legislation, because outer space is intrinsically analogous to cyberspace. Both are extremely vast areas of shared information exchange. Furthermore, international exchanges in both areas cannot be nationalized under international law, making them difficult to police. So far there are no rules on how to use outer space during armed conflict (with the exception that nuclear weapons are banned in outer space), which means that space law provides no guidance on how cyberspace should be used during armed conflict. Moreover, since cyberspace is *already* being used during armed conflict, as the case with Georgia demonstrates, there is a pressing need to answer this question, which space law cannot do.

Yet there is another approach. Thomas Wingfield suggests:

> Rather than banning only the most egregious cyber use [as space law recommends]…it may be more thorough to regulate all hacking that could become a cyber attack. The Antarctic Treaty System (ATS) provides a fruitful analogue of a commons area that has gone the extra step of banning *all* military activities.[73]

This kind of analogy may end up hurting more than helping, as it may prove better at times to take out an enemy cyber network than to commit a physical attack, which would likely result in a greater amount of collateral damage. It would also stifle the innovative nature of technology.

---

[72] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375.

[73] Thomas C. Wingfield, "International Law and Information Operations," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press and Potomac Books, Inc., 2009), 526.

Turning then to International Human Rights Law and International Humanitarian Law, Kenneth Watkin notes that both "are rooted in respect for human values and the dignity of the human person—first principles that are applicable at all times and from which no derogation is permitted."[74] Some cyber attacks, however, violate one of the most important tenets of International Human Rights Law: the right to privacy. Watkins warns, "Precisely because states and individual hackers can hide behind the privacy the Internet affords, regulating cyberspace also hazards on intruding on the privacy of innocents."[75] U.S. policy does regulate federal cyber activities; however, this is not necessarily true of other nations. Furthermore, much more is at stake in cyber attacks than a violation of privacy, which is often difficult to prove as it is.

But while all of these existing conventional analogies have validity, they all fall short of providing a necessary legal framework to regulate cyber attacks. The best current governance of nation-state cyber attack may in fact be the law of war, or law of armed conflict, itself. Looking specifically at nation-state cyber attacks, the Department of Defense Office of the General Counsel advises:

> There are novel features of information operations that will require expansion and interpretation of the established principles of war…The law of war is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations.[76]

C. THE LAW OF ARMED CONFLICT

Scott Shackelford is one scholar in agreement with the law of armed conflict's jurisdiction over nation-state cyber aggression. He argues:

---

74 Kenneth Watkin, "Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict," American Society of International Law, http://74.125.155.132/search?q=cache:CSPE4o2JdroJ:www.asil.org/ajil/watkin.pdf+Kenneth+Watkin,+Controlling+the+Use+of+Force:+A+Role+for+Human+Rights+Norms+in+Contemporary+Armed+Conflict,&cd=1&hl=en&ct=clnk&gl=us&client=firefox-a.

75 Ibid.

76 Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations, December 1999, http://www.cs.georgetown.edu/~denning/infosec/DoD-IO-legal.doc.

> Cyber attack should be judged according to the principles of the law of armed conflict (LOAC) and the UN Charter, encompassing both *jus ad bellum* (law governing the legality of going to war) and *jus in bello* (law governing behavior during war) with the understanding that new analytical work is needed to understand how these principles do or should apply to cyberweapons.[77]

Though both deal with the use of force, the former specifies *when* that force may be applied, while the latter specifies *how* it should be applied.

1. Jus Ad Bellum

Jus ad bellum is explicitly codified in the United Nations Charter and specifies the conditions under which member states may use force against each other. The most relevant parts of the Charter to state cyber attacks are Articles 2(4), 39, and 51. These articles have been respected by nations since the U.N. Charter's inception, and they continue to be followed today. These basic *jus ad bellum* laws, therefore, remain a necessary foundation for any further development.

Article 2(4) forbids states from using force against other states; however, in the event that nation-states violate this law, Article 39 grants the United Nations Security Council authority for responding to threats and acts of aggression. Along with these two provisions, though, there is also an inherent right to national self-defense. Article 51 of the U.N. Charter explicitly permits states to undertake offensive action for purposes of self-defense, or even anticipatory self-defense. Professor Dorothy Denning summarizes:

> …the UN Charter prohibits states from using force (Article 2(4))…except when conducted in self-defense (Article 51) or under the auspices of the Security Council (Article 39)…States have a moral right to defend themselves against acts and threats of aggression, but they do not have the right to engage in unprovoked aggression.[78]

States that have signed onto the Charter have agreed to abide by these rules when waging conventional wars.

---

[77] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities* (Washington, D.C.: The National Academies Press, 2009), 3–20.

[78] Dorothy E. Denning, The Ethics of Cyber Conflict, in *The Handbook of Information and Computer Ethics* eds. K. E. Himma and H. T. Tavani, 4 (Hoboken, NJ: Wiley, 2008).

To judge any nation-state cyber attack scenario by the *jus ad bellum* principles laid out by the U.N. Charter, it is first necessary to further articulate the idea of "use of force" as it applies to cyber attacks. As with all weapons, cyber attacks that present a use of force violate Charter rules if not done under Articles 39 or 51.

Michael Schmitt, Professor of International Law and Director of the Program in Advanced Security Studies at the George G. Marshall European Center for Security Studies in Germany, has devised a series of measures by which to judge cyber attacks. Collectively, these measures can be utilized to determine if a nation-state cyber attack amounts to a "use of force," thereby violating customarily acknowledged *jus ad bellum* if not undertaken as authorized by the U.N. Security Council, or in self-defense. The criteria, as articulated by Schmitt, and later Thomas Wingfield and Dorothy Denning, stated: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[79]

Severity refers to people killed or wounded and property damage. Cyber attacks that cause greater human casualties and/or property damage are more likely to be considered "uses of force."

Immediacy is the time it takes for the consequences of an operation to take effect. The idea here is that instantaneous consequences are indicative of cyber attacks that qualify as uses of force.

Directness is the relationship between an operation and its effects. The easier it is to directly attribute a cyber attack to certain effects, the better chance that cyber attack has of being viewed as a use of force.

Invasiveness refers to whether an operation involved crossing borders into the target country. It is generally understood here that cyber attacks that cross physical borders have a higher chance of being understood as uses of force, rather than those that stay within a nation's territorial boundaries.

[79] The following definitions are those of Professor Dorothy Denning in the previously cited work, as paraphrased from Michael Schmitt and Thomas Wingfield's earlier work.

Measurability is the ability to measure the effects of an operation. Uses of force usually involve quantifiable damage, a standard by which cyber attacks are also judged, though sometimes not easily.

Presumptive legitimacy refers to whether an operation is considered legitimate within the international community. Cyber attacks that appear to be a use of force would clearly violate the U.N. Charter Article 2(4), unless they are undertaken for reasons of self-defense (U.N. Charter Article 51), or as authorized by the Security Council (Article 39). The response of the international community to a particular nation-state cyber attack can be indicative of its presumptive legitimacy.

Responsibility refers to the degree to which the consequence of an action can be attributed to a state as opposed to other actors. The degree to which cyber attacks are clearly attributable to nation-states demonstrates whether or not those attacks fall under the "use of force" category. Obvious state cyber aggression is more likely to be regarded as a use of force than nonstate cyber attacks.

The U.N. Charter, along with Schmitt's criteria, however, only serve to regulate nation-state cyber attacks before war has been waged. Once force has been used, and war has begun, cyber attacks are then judged by different standards. They then fall under the purview of *jus in bello*.

2. Jus In Bello

Once armed conflict has begun, each nation's military forces are subject to long-standing *jus in bello* constraints. Their conduct during war is governed by legislation produced at the Hague Conferences, the Geneva Conventions, and customary international law. As these rules govern state conduct during war at all times, these same legal conventions therefore apply to nation-state cyber attacks during counterterrorism operations as well.

The commonly recognized principles of *jus in bello*, or the law governing the conduct of war, are: military necessity, proportionality, perfidy, distinction, neutrality, and discrimination. The United States Department of Defense then also adds the

principle of superfluous injury to this list. These standards can be used to regulate cyber attacks as a military weapon, the same way they do for kinetic weapons.

1. *Distinction of combatants from noncombatants*: Only members of a nation's regular armed forces may use force, and they must distinguish themselves and not hide behind civilians or civilian property.

2. *Military necessity*: Targets of attack should make a direct contribution to the war effort or produce a military advantage.

3. *Proportionality*: When attacking a lawful military target, collateral damage to noncombatants and civilian property should be proportionate to military advantage likely to be achieved.

4. *Indiscriminate weapons:* Weapons that cannot be directed with any precision, such as bacteriological weapons, should be avoided.

5. *Superfluous injury:* Weapons that cause catastrophic and untreatable injuries should not be used.

6. *Perfidy:* Protected symbols should not be used to immunize military targets from attack, nor should one feign surrender or issue false reports of cease-fires.

7. *Neutrality:* Nations are entitled to immunity from attack if they do not assist either side; otherwise, they become legitimate targets.[80]

To the extent that nation-state cyber attacks defy any of the *jus in bello* principles outlined above, they then violate existing international law. The same holds true when state cyber attacks breach the tenets of *jus ad bellum*. The question then arises, are these long-standing international laws of armed conflict enough to regulate nation-state cyber attacks, including cyber attacks against terrorists?

[80] Dorothy E. Denning, The Ethics of Cyber Conflict, *The Handbook of Information and Computer Ethics* (K. E. Himma and H. T. Tavani, eds.), Wiley, 2008, 8. Denning cites here a summarized list offered by the Department of Defense Office of the General Counsel.

The National Research Council finds:

> The conceptual framework that underpins the U.N. Charter on the use of force and armed attack and today's law of armed conflict provides a reasonable starting point for an international legal regime to govern cyber attack. However, those legal constructs fail to account for non-state actors and for the technical characteristics of some cyber attacks.[81]

The challenges that these new aspects of war present to the long-standing international laws outlined above will become clear in the next chapter on potential nation-state cyber attacks during counterterrorism operations.

[81] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities* (Washington, DC: The National Academies Press, 2009), 32.

IV. FUTURE ATTACK SCENARIOS AND THEIR LEGAL ANALYSES

After examining where current international law stands on the issue of nation-state cyber attacks in counterterrorism operations, it is clear that no comprehensive legislation exists to respond to terrorists. The 1998 Rome Statute may also hold relevance for all nation-state counterterrorism operations in the future, including cyber attacks. Yet that possibility will first require a consensus definition of "terrorism," which may not happen for some time. On the broad issue of military conduct, Lieutenant General Keith Alexander, Director of the National Security Agency and Nominee for Commander of the United States Cyber Command has testified, "Per DoD guidance, all military operations must be in compliance with the laws of armed conflict—this includes cyber operations as well."[82] Yet in order to examine if, and how, these laws should evolve to best meet this new form of attack, it is necessary to first look at cyber attacks that could possibly be seen in future counterterrorism operations. Potential attack scenarios to collect intelligence, sow deception, cyber-herd, and attack and destroy will follow. Each scenario will also include a legal analysis, based on the application of existing *jus ad bellum* and *jus in bello* regulations. The former will rely on Michael Schmitt's criteria to determine nation-state use of force, which is only legal in self-defense (Article 51) or as sanctioned by the United Nations Security Council (Article 39). The latter will rely on long-established principles of customary and conventional law, as formally articulated by the Department of Defense.

A. ATTACK SCENARIO #1: CYBER EXPLOITATION

Nation-states, if they choose to conduct cyber attacks as part of their counterterrorism operations, will very likely do so for the purpose of collecting intelligence. This scenario is not considered an attack, but rather an "exploit." The National Research Council refers to "espionage conducted by or through the use of a

82 Keith Alexander, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command," *Washington Post*, http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf.

computer" as "cyber exploitations."[83] In order to collect intelligence, nations can use many cyber techniques to hack into adversary computer systems and monitor the information exchange. As they are considered espionage, these activities are currently legal under international law.

Country A will use a combination of sniffers, keyloggers and routing attacks on terrorist group X in order to collect intelligence. Country A will begin by inserting sniffer software onto the computers of major players within group X. This software will scan Internet traffic, looking for certain programmed words and phrases. In addition, country A will also place keylogger software on those same computers in order to record the keystrokes of the major players, thereby giving country A passwords to secure sites, email and chat rooms. Finally, country A will add a routing attack to its intelligence collection attack scenario. By redirecting Internet traffic to pass through their own networks, country A can monitor group X's traffic flow.

1. Legal Analysis

As mentioned above, cyber exploitation is not currently a violation of international law, so *jus ad bellum* and *jus in bello* do not apply. If the target computers are located in the United States, then U.S. law governs what the intelligence collection agencies can do. Cyber espionage, if conducted against target computers outside the US, may violate domestic laws in foreign countries.

B. ATTACK SCENARIO #2: DECEPTION

Related to intelligence collection is the idea of deception. Countries may choose to impersonate certain terrorist group members to relay their own information. Nation-states will likely commit such deceptive cyber attacks using a variety of different tactics. The idea would be to fool terrorist group members into believing they are interfacing

[83] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities* (Washington, D.C.: The National Academies Press, 2009), 261.

with trusted people and Web activity, the ultimate goal being to draw terrorists into giving up information that a nation can exploit for their own advantage.

In this scenario, country A will commit identity theft against terrorist group X. Country A can go about this is a number of ways, but they will likely choose to do so using keylogger spyware to gain the login information of one group X member, and they may then undertake a phishing attack on another group X member to gain his/her login information. Once country A has the login information of both members, they can not only view the individual activity of each, but also use the login information they gained to impersonate the terrorists through email and in chat rooms. Once inside the various Web forums, country A can leak false information and sow doubt amongst group X members. This cyber identity theft scenario would also likely damage group X morale if one of the individuals personified was a group X leader or high-ranking member.

1. Legal Analysis

Looking at the *jus ad bellum* laws, this scenario of cyber deception seemingly resembles force under Schmitt's evaluation criteria of invasiveness, measurability, and presumptive legitimacy. Though not as invasive as sending troops and other personnel, this attack raises issues of invasiveness by invading terrorists' Web activity. On measurability, country A's deception can be measured by the number of accounts impersonated or the percentage of messages that sow suspicion and/or cast doubt, for example; however, it would be difficult to measure the indirect effects. These deceptive attacks are also a concern for presumptive legitimacy if conducted prior to any armed attack, since they are unlikely to be regarded as legitimate at that time. On the other hand, the criterion of responsibility does not suggest use of force, since this attack could be attributed as easily to nonstate actors as it could to nation-states. The level of severity also does not suggest force, as no one is killed, and the property damage is likely minimal. And while this deceptive cyber attack scenario includes effects that are immediate and direct, both of which indicate a use of force, there are also larger indirect effects that are not immediate. Some of Schmitt's criteria, then, suggests force, but others do not, leaving an ambiguous conclusion on *jus ad bellum*.

If undertaken during war, this deceptive cyber attack scenario falls under the purview of *jus in bello*, which country A largely follows here. There is distinction of combatants from noncombatants, and no indiscriminate weapons are used or superfluous injuries incurred during this attack. This deceptive cyber attack is also of military necessity, since information garnered will be used to advance Country A's counterterrorism operation. There is also no collateral damage, so proportionality is not called into question. Neutrality is a concern, since the packets may transit neutral countries and the Web/email servers used during impersonation may be located in neutral countries. Country A, in conducting a deceptive attack, must also be careful not to cross the lines of perfidy while masquerading as certain individuals and generating phony Web sites if it is to remain within the regulations of international law. Feigning a cease-fire from a group X leader, for example, would violate the perfidy requirement.

In addition to *jus ad bellum* and *jus in bello* considerations, this attack scenario then also raises a unique concern for international law: identity theft by a nation-state. It is necessary here for country A to use caution when undertaking what is regularly considered criminal activity, yet is no current violation of international law.

C. ATTACK SCENARIO #3: CYBER-HERDING

To have the greatest impact as a counterterrorism tool, an offensive cyber-herding attack would be best conducted by an industrialized nation with the knowledge and capability to replicate the Web activity of the adversary terrorist group. In this case, the terrorist group attacked with such a strategy would likely be one with a great deal of Web activity in order to maximize the attack effort.

In this scenario, country A would choose to employ such a cyber-herding strategy against terrorist group X. In the gathering phase, country A finds that group X is a large, decentralized network. So, country A will begin by carefully analyzing the network structure to discover which nodes and links are most important. Identifying where the hubs and connectors are will show country A where to insert themselves into the network as virtual players, and where to focus their energy in the construction phase, saving country A time and energy, and meanwhile gaining the maximum impact from the attack.

Since country A then now knows where to focus their efforts, they will do so in the construction phase by choosing to make replicas of group X's most influential and dangerous Web sites, chat rooms, and Darknet environments (private virtual networks where users connect only to people they trust through email, file sharing, chat, instant messenger, and streaming video services).[84] Country A will then forward what has been created to its virtual players in the network to pass to the identified hub and connector people in group X. Once the phony sites, chat rooms, and Darknet environments have picked up in popularity among group X members, country A will begin a slow demolition of group X's Web sites and forums. Country A will simultaneously subtly change the message in the Web sites and forums they created to raise doubts and questions about group X, and then finally concentrate and demolish their own phony Web activity, having already taken down group X's original sites and forums.

1. Legal Analysis

This cyber-herding attack does pose some challenges for international law. Turning first to the rules of *jus ad bellum*, several considerations suggest this cyber attack scenario may be regarded as a use of force. This is particularly true of Schmitt's criteria of invasiveness, presumptive legitimacy, and responsibility. As with the deceptive scenario, invasiveness is not as great in this cyber-herding attack as it would be with a kinetic attack. Yet it remains an important issue since country A will be invading terrorists' Web activity. This particular cyber-herding attack may resemble force given Schmitt's presumptive legitimacy consideration, as other nations will likely not consent to any attack conducted prior to armed conflict. This attack also looks like force using the responsibility standard, since the extent of the attack suggests a nation-state attacker, country A in this scenario. Cyber-herding as it is used here is also direct, though its indirect effects are also significant. In addition, there is high measurability since the number of group X Web sites ultimately demolished can be counted with relative ease. It is not immediate, since it will take time to get the group X to accept the phony sites and

[84] David B. Moon, "Cyber-Herding: Exploiting Islamic Extremists Use of the Internet" (Monterey, CA: Naval Postgraduate School, 1997).

then move over to them, meanwhile continually creating new sites. The severity of this cyber-herding attack scenario is also low, but on balance, the operation looks more like force than the preceding one.

If war has already begun, then *jus in bello* laws pertain. In this case, the *jus in bello* rules are largely followed, since the cyber-herding scenario meets almost all of the long-established standards. As with the deceptive nation-state cyber attack scenario, distinction, indiscriminate weapons, and superfluous injuries are not issues here. There is also no collateral damage to defy proportionality. The cyber-herding attack here meets military necessity, since the reduced number of group X Web activity are intended to aid country A's counterterrorism efforts. In addition, perfidy is not a concern, since the cyber-herding technique involves creating mirror image negative Web activity, not impersonating positive protected symbols. Neutrality is an even larger issue than in the deceptive attack scenario, since cyber-herding ends by taking down the original Web sites, Web sites, which may be hosted in neutral countries.

This cyber-herding scenario, however, does raise an interesting question for international law not covered by either *jus ad bellum* or *jus in bello*. Here, country A conducts credible anti-country A Web activity to attract terrorists. It is not the ends that are of concern here, but rather the means used to achieve those ends. The degree to which it is legal for governments to engage in seditious acts for the greater good is a gray area in international law, and it is an issue that would arise in all potential nation-state cyber-herding attacks.

D. ATTACK SCENARIO #4: ATTACK AND DESTROY

Nations-states may also choose to implement cyber attacks to degrade the quality of terrorist groups' Web activity, or even to shut down that activity entirely. Country A, here, wishes to both decrease the influence of terrorist group X's Web activity, and to reduce the overall amount of that activity as well. To do this, they will employ a variety of techniques, including malware, DOS attacks, Web defacements, and legitimate ISP shutdowns.

Country A will begin by inserting malware onto group X members' computers. Their cyber attack will start with phony spam emails that install the malicious software on the targeted computer systems. Once the malware is installed, country A may choose to only damage infected computer systems, or they may decide to entirely take down those systems. They could even start with damage, and then move to complete destruction later. In addition to installing malware, country A may conduct DOS attacks against group X computers, devastating their ability to function. In conducting DOS attacks, country A will have to be careful not to inadvertently attack innocent third parties hosting the targeted Web sites and email. Country A may also choose to use malware and DOS attacks only on certain group X computer systems, while leaving others intact. Country A could even deface some of group X's Web sites, changing the content to be detrimental to group X. Finally, country A may decide to contact ISPs to shut down designated group X sites entirely, precluding group X's ability to renew those specific Web sites in the exact same way.

1. Legal Analysis

Turning to the legality of this attack-and-destroy cyber attack scenario, it is necessary to once again look at *jus ad bellum* law, as well as *jus in bello* regulations once conflict has begun.

Under Schmitt's evaluation of immediacy, directness, invasiveness, measurability, and presumptive legitimacy, these cyber attack techniques give reason to be labeled as a use of force. Immediacy is at play here, since attack damage is instant, no matter when group X notices the damage. Furthermore, directness is high since the damage done is directly related to the attack conducted. Without the cyber attack, there is no damage. As with the other attack scenarios, invasiveness is also high (though still not as great as with a kinetic attack). Reaching out to penetrate computer systems across the globe crosses national boundaries is cause for concern under international law. Measurability can be managed by looking at the number of Web sites taken down, or even the amount of activity conducted. Presumptive legitimacy is another concern if this cyber attack-and-destroy scenario is carried out prior to any armed attack. The severity

of this attack is low, which would point to no use of force. Though this cyber attack scenario is undertaken by a nation-state, it could be attributable to a nonstate actor, also suggesting no use of force under Schmitt's responsibility consideration. Given evaluation of all Schmitt's criteria as a whole, this cyber attack may be labeled as a use of force, a violation if not done in self-defense or as sanctioned by the United Nations Security Council.

If armed attack has begun, *jus in bello* standards apply. By and large, country A's cyber attack here meets the *jus in bello* criteria established by conventional and customary international law. Neutrality remains a concern, since third parties probably host group X Web sites and e-mail, which may be in neutral countries. So, anything that defaces Web sites or involves attacking them or taking them down, may involve neutral countries. And though property damage and people killed may be minimal, there could still be collateral damage. A DOS attack against a Web site could affect all the Web sites hosted by the Internet Service Provider (ISP) on the same Web server. This attack-and-destroy cyber scenario then meets the same *jus in bello* regulations as the previous two: distinction of combatants from noncombatants, no indiscriminate weapons, and no superfluous injuries. Finally, military necessity is met by the decrease in group X Web activity resulting from this attack-and-destroy cyber scenario, and there is no problem with perfidy since impersonation is not a part of this cyber attack scenario.

As mentioned earlier, a unique international law area to be cautious of with this cyber attack scenario is avoiding innocent third parties. The inherent connectivity of the Internet makes this more difficult to do than during kinetic warfare, but no less necessary.

Excluding the cyber-exploitation scenario then, each of the preceding cyber attack scenarios, has presented challenges to either or both of existing *jus ad bellum* and *jus in bello* rules. There are also new areas of concern for international law, arising from the use of cyber technology to combat terrorists.

E. THE NEW AREAS OF CONCERN

The new areas of concern highlighted in the preceding scenarios fall outside the realm of the law of armed conflict. They present challenges that arise from the nature of

a modern warfare being fought using a new weapon on an unconventional battlefield. Deciding how to regulate these new concerns is critical for the future of war; however, international law can evolve to meet these challenges only after greater examination of their distinctive natures.

Duncan Hollis has particularly noted two different problems with the law of armed conflict vis-à-vis cyber attacks, issues that have resulted in many of the new areas of concern outlined above. First is what he refers to the "translation problem."[85] This is seen first and foremost with the idea of collateral damage. The established law of armed conflict only takes into account the immediate death and destruction of kinetic attacks, not the economic and digital damage of cyber attacks. This is exactly why the *jus in bello* standard of proportionality, as well as Schmitt's *jus ad bellum* evaluation criteria of severity, were not big concerns in any of the nation-state cyber attack scenarios above. There was never much collateral damage as Schmitt currently defines it.

The second problem Hollis sees with LOAC gives way to another diverse set of new concerns: the state-on-state focus.[86] The law of armed conflict does not take into account state conduct during confrontations with nonstate actors, including counterterrorism operations. It does not account for the changing rules or new fighting strategies. A gray area has arisen here in which nation-states may use what is domestically considered criminal activity to combat terrorists with no collateral damage. The cyber attack scenarios above, for example, demonstrate country A undertaking what would ordinarily be considered identity theft and sedition in order to carry out their cyber deception and cyber-herding attacks, respectively. These crimes are prosecutable under domestic law, but are they beneficial internationally in order to minimize the number of people killed and the amount of property damage that would otherwise occur because of terrorism?

---

85 Duncan B. Hollis, "New Tools, New Rules: International Law and Information Operations," in *Ideas as Weapons: Influence and Perception in Modern Warfare*, eds. G. David and T. McKeldin, 59–62 (Dulles, VA: Potomac Books, Inc., 2009).

86 Ibid.

Finally, there is an "interconnectivity problem." The interconnected nature of the Internet makes it almost impossible to avoid involving neutral nations and innocent third parties during nation-state cyber attacks, the negative repercussions of the latter already being seen in past and present kinetic wars. Both of these issues prove problematic for the existing laws of war, which seek, above all, to separate combatants from noncombatants. International law exists to protect both during war, but would they in fact be better off facing the tangential damage of cyber attacks, rather than the direct damage of kinetic warfare? These are all important considerations to face before there can be any evolution of international law to meet these new challenges.

This chapter has demonstrated that there are obvious challenges to current international regulation of nation-state cyber attacks by the law of armed conflict. There are also new issues of concern for any future evolution of international law. The question is: What is the best response to the challenges nation-state cyber attacks in counterterrorism operations present to international law?

V. CONCLUSION

As demonstrated by Chapter IV, there are inherent ambiguities with the current means of internationally regulating nation-state cyber attacks in counterterrorism operations. Additional questions were then raised regarding new areas of concern for international law. In many ways, flaws of evaluation and enforcement are behind these issues, and they must be addressed to allow better international regulation of these kinds of attacks.

A. EVALUATION

The cyber scenarios described in Chapter IV represented possible nation-state cyber attacks during counterterrorism operations. Pre-existing conventional and customary international law was used to conduct legal analysis, but any legal analysis on the subject of such cyber attacks is difficult, given the new technology and previous state-to-state focus. This is demonstrated in part by the use of Michael Schmitt's evaluation criteria to determine uses of force.

Schmitt employed his "use of force" evaluation criteria to examine computer network attacks (CNAs) that were either obvious uses of force, or were clearly less severe measures. As demonstrated in the Chapter IV, nation-state cyber attacks in counterterrorism operations will likely fall into neither category. The new technology makes it probable that these attacks will blur the line between uses of force and less extreme actions by exhibiting characteristics of both.

This brings up a crucial second point: it is not clear that Schmitt's criteria—as they are defined and understood—aptly distinguish cyber attacks that constitute force from those that do not. Cyber attacks, by their nature, may frequently come out low on many of Schmitt's criteria, relative to kinetic uses of force. This is the case, for example, with invasiveness and severity when there is no collateral damage. Invasiveness may be digital rather than physical, and cyber attacks may in fact be severe, without creating the physical damage and destruction that Schmitt emphasizes.

Given the changing nature of warfare, Schmitt's criteria for evaluation presents difficulties for "use of force" determinations. New technology and new belligerents stymie attempts to evaluate whether nation-state cyber attacks in counterterrorism operations constitute uses of force. Not having adequate force evaluation then makes gauging the legality of these attacks using dated international regulation even more difficult. Being able to determine the legality of an attack is a critical component of warfare, as is enforcement when such attacks are determined illegal.

B. ENFORCEMENT

Enforcement is a critical response if nation-state cyber attacks in counterterrorism operations were to violate existing international law. The United Nations, the International Court of Justice, and the International Criminal Court are the current enforcers of international law; however, certain aspects of these modern attacks mentioned earlier will likely challenge their enforcement authority and functionality. If this is the case, even after evaluation is improved and international law amended, insufficient enforcement would then leave no motivation for nation-states to follow these new rules.

The United Nations has long been the main source of international law enforcement. In the event of acts of aggression or breaches to the peace, the Security Council may exercise its Chapter VII right to adopt binding international law resolutions that call for anything from economic sanctions to military action. Should the Security Council become deadlocked, as has occurred historically during the Cold War, for example, the General Assembly can also approve enforcement resolutions, though they are not considered binding. In addition, nation-states themselves have the option to take their case to the United National International Court of Justice (ICJ); however, this last option requires the mutual consent of both parties, which is not always easy to obtain. This would be especially true if one party were not a traditionally understood state, as is the case with al-Qaeda, for example. Furthermore, while ICJ judgments are considered

binding, several years may pass before they are rendered, and there remains no armed mechanism to truly enforce them. In most cases, therefore, ICJ judgments remain no more than advisory opinions.[87]

The International Criminal Court (ICC) was recently formed as a judicial arm of international law. According to their Web sites, pursuant to the Rome Statute, "the Prosecutor can initiate an investigation on the basis of a *referral* from any State Party or from the United Nations Security Council. In addition, the Prosecutor can initiate investigations *proprio motu* on the basis of information on crimes within the jurisdiction of the Court received from individuals or organisations ("*communications*")."[88] Their record indicates:

> To date, three States Parties to the Rome Statute—Uganda, the Democratic Republic of the Congo and the Central African Republic—have referred situations occurring on their territories to the Court. In addition, the Security Council has referred the situation in Darfur, Sudan—a non-State Party.[89]

States must first agree to be party to the ICC, and the United States, for example, has not yet done so, exemplifying the problem. Furthermore, state adversaries in this case are non-state actors. In addition, the ICC exists to try only the gravest crimes, and is considered a court of last resort, neither of which would pertain to the large majority of nation-state cyber attacks in counterterrorism operations. Even if so, the ICC also suffers from the lack of any means of armed enforcement.

C. CONCLUSION

1. Findings and Policy Implications

This thesis has studied existing international law as it applies to nation-state cyber attacks in counterterrorism operations. It has found that the application of existing laws

---

87 United Nations, "International Court of Justice, United Nations, http://www.icj-cij.org/court/index.php?p1=1&PHPSESSID=633d3b8ae47f7c208b91b7833aae8ebd.

88 The International Criminal Court, "Situations and Cases," The International Criminal Court, http://www.icc-cpi.int/Menus/ICC/Situations+and+Cases/.

89 The International Criminal Court, "Situations and Cases," The International Criminal Court.

poses several challenges, including the difficulty of relating cyber attacks to customary interpretations of what constitutes force. Yet it is not enough to devise better force evaluation criteria. Nation-state cyber attacks are a unique military weapon whose best response may require entirely new legal principles. These principles would regulate cyber attacks as they relate to each other, and not to kinetic uses of force. They would be as applicable to nation-states, as they would be to individuals and groups or organizations. Above all, these new international legal principles would account for economic and digital "damage," state-on-nonstate attacks, and the inevitable interconnectivity and, therefore, involvement of innocent third parties.

The policy implication of such a monumental task is one of international activism. To codify new legal principles on the use of such an enigmatic, but threatening, new weapon will require an enormous international effort to increase awareness of cyber attacks, foster understanding of their unique significance, and reach consensus on their regulation. The best method may be to begin discussion at the United Nations, using the already accepted laws and norms of war to construct a basic framework for new cyber-specific legal principles that also addresses the new areas of concern raised above.

On enforcement, there have already been attempts to better regulate crimes in cyberspace, though they remain focused on traditionally understood domestic crimes, and primarily on nonstate actors. Leading the effort is International Convention on Cybercrime. The Convention on Cybercrime was adopted in 2001 by the Council of Europe, a consultative assembly of 43 countries, based in Strasbourg. The Convention, effective July 2004, is the first and only international treaty to deal with the breaches of law:

> …over the Internet or other information networks. Thirty countries, including the United States, have signed on to the Cybercrime Convention. However, there is more work to be done. The Convention requires state signatories to "update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.[90]

[90] Council of Europe, "Convention on Cybercrime," Council of Europe, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

The United States has, at present, adopted only the provisions that are in keeping with its existing federal law, being particularly careful not to challenge the U.S. Constitution's First Amendment. This reveals that sovereignty remains a primary concern, and will continue to be at the forefront of international response discussions for some time to come. Yet, more flexibility will be needed from all nations in the future in order to make this or any other international cyber convention effective.

There are different policy implications here that can be used to achieve the objective of greater enforcement. The United Nations could include nonstate actors in ICJ adjudication, which would be both advantageous and disadvantageous, as it would subject nonstate actors more to international law as legitimate international players. Nation-states could also come together to create a new enforcement mechanism, similar to the ICC, which would allow adjudication between state and nonstate actors, but for crimes less than grave. Countries would then need to put their full weight behind whichever international institution is responsible for enforcement of these attacks. This may prove difficult, as countries that sign on may then themselves become subject to enforcement; however, nation-states may have been just frightened enough by the Georgian attacks to consider supporting enforcement worthwhile.

There is still a critical place in modern combat for the age-old law of armed conflict; however, it must be updated to allow international law greater governance over new weapons and new battlefields. Improving force evaluation and enforcement mechanisms, are essential first steps to future governance of nation-state cyber attacks in counterterrorism operations. As warfare modernizes, so too must the regulation of its conduct.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alexander, Keith. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." *Washington Post*. http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf. Accessed April 20, 2010.

Asset Recovery Knowledge Centre. "International Convention for the Suppression of the Financing of Terrorism, 1999." International Centre for Asset Recovery. http://www.assetrecovery.org/kc/node/9d9db21c-a349-11dc-bf1b-335d0754ba85.0;jsessionid=03FFFDE24A3F752DFC3E6B193031D786. Accessed March 11, 2009.

Audiovisual Library of International Law. "Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents." United Nations. http://untreaty.un.org/cod/avl/ha/cppcipp/cppcipp.html. Accessed March 22, 2009.

Brookes, Peter. "The Cyberspy Threat: Foreign Hackers Target Military." Family Security Matters. http://www.familysecuritymatters.org/publications/id.3103/pub_detail.asp. Accessed June 2, 2009.

Byman, Daniel. *The Five Front War: The Better Way to Fight Global Jihad*. Hoboken, NJ: John Wiley & Sons, Inc., 2008.

CIGI Online. "Annan Proposes Definition of Terrorism." The Centre for International Governance Innovation. http://www.igloo.org/community.igloo?r0=community&r0_script=/scripts/announcement/view.script&r0_pathinfo=%2F{7caf3d23-023d-494b-865b-84d143de9968}%2FAnnouncements%2Fciginews%2Fannanpro&r0_output=xml. Accessed March 20, 2009.

Collins, Susan M. Paper presented to the United States Senate Committee on Homeland Security and Government Affairs. Washington, D.C., April 28, 2009.

Committee Documents. "Implementation of the International Convention for the Suppression of Terrorist Bombings and the International Convention for the Suppression of the Financing of Terrorism." United States House of Representatives. http://commdocs.house.gov/committees/judiciary/hju76122.000/hju76122_0.htm#1. Accessed March 18, 2009.

Council of Europe. “Convention on Cybercrime.” Council of Europe. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. Accessed May 2, 2010.

Cyberspace and Information Operations Study Center. “Computer Network Operations & Network Warfare Operations.” Air University. http://www.au.af.mil/info-ops/netops.htm. Accessed April 14, 2010.

Denning, Dorothy E. “Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.” Georgetown University. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. Accessed June 2, 2009.

———. “The Ethics of Cyber Conflict.” In *The Handbook of Information and Computer Ethics*. Eds. K. E. Himma and H. T. Tavani. Hoboken: John Wiley & Sons, Inc, 2008.

———. “Terror’s Web: How the Internet Is Transforming Terrorism.” In *Handbook on Internet Crime*. Eds. Yvonne Jewkes and Majid Yar. Portland, OR: Willian Publishing, 2009.

Department of Defense Office of General Counsel. An Assessment of International Legal Issues in Information Operations. December 1999. http://www.cs.georgetown.edu/~denning/infosec/DoD-IO-legal.doc. Accessed May 18, 2009.

Eedle, Paul. “Terrorism.com,” *Guardian*, July 17, 2002. http://www.guardian.co.uk/print/0,3858,4462872-103680,00.html. Accessed May 20, 2009.

Emsisoft. “Dictionary of Computer Security Terms.” http://www.emsisoft.com/en/kb/articles/tec080424/. Accessed May 12, 2010.

Europa. “Activities of the European Union: Summary Legislation.” http://europa.eu/scadplus/leg/en/lvb/l27080.htm. Accessed May 2, 2010.

Flory, Maurice. “International Law: An Instrument to Combat Terrorism.” In *Terrorism and International Law*. Eds. Rosalyn Higgins and Maurice Flory. New York: Routledge, 1997.

Freestone, David. “International Cooperation Against Terrorism and the Development of International Law Principles of Jurisdiction.” In *Terrorism and International Law*. Eds. Rosalyn Higgins and Maurice Flory. New York: Routledge, 1997.

Gertz, Bill. “China blocks U.S. from Cyber Warfare.” *The Washington Times*. http://washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/. Accessed June 12, 2009.

Greenberg, Lawrence, Goodman Seymour E., and Soo Hoo, Kevin J. *Information Warfare and International Law*. Washington, DC: National Defense University, 1998.

Hollander, Yona. “Prevent Web Site Defacement.” Internet Security. http://www.mcafee.com/us/local_content/white_papers/wp_2000hollanderdefacement.pdf. Accessed May 13, 2010.

Hollis, Duncan B. “New Tools, New Rules: International Law and Information Operations.” In *Ideas as Weapons: Influence and Perception in Modern Warfare*. Eds. G. David and T. McKeldin, Dulles, VA: Potomac Books, Inc., 2009.

The International Criminal Court. “Situations and Cases.” The International Criminal Court. http://www.icc-cpi.int/Menus/ICC/Situations+and+Cases/. Accessed May 29, 2010.

International Maritime Organization. “Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988.” International Maritime Organization. http://www.imo.org/Conventions/mainframe.asp?topic_id=259&doc_id=686. Accessed March 12, 2009.

Inventory of International Nonproliferation Organizations and Regimes. “Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal Convention).” Center for Nonproliferation Studies. http://209.85.173.132/search?q=cache:4X_Gzst56G4J:www.nti.org/e_research/official_docs/inventory/pdfs/civair.pdf+the+1971+Montreal+Convention+for+the+Suppression+of+Unlawful+Acts+Against+Aircraft+Safety&cd=3&hl=en&ct=clnk&gl=us&client=firefox-a. Accessed March 14, 2009.

———. “Convention on the Marking of Plastic Explosives for the Purpose of Detection.” Center for Nonproliferation Studies. http://209.85.173.132/search?q=cache:VKJOWWye12QJ:www.nti.org/e_research/official_docs/inventory/pdfs/pexplo.pdf+The+1991+Convention+on+the+Making+of+Plastic+Explosives&cd=2&hl=en&ct=clnk&gl=us&client=firefox-a. Accessed March 12, 2009.

———. “Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation.” Center for Nonproliferation Studies. http://209.85.173.132/search?q=cache:feUTsOWRdOIJ:www.nti.org/e_research/official_docs/inventory/pdfs/airport.pdf+The+1988+Protocol+on+the+Suppression+of+Unlawful+Acts+of+Violence+at+Airports&cd=8&hl=en&ct=clnk&gl=us&client=firefox-a. Accessed March 11, 2009.

Laursen, Andreas. *Changing International Law To Meet New Challenges: Interpretation, Modification And The Use Of Force*. Portland, OR: Djoef Publishing, 2006.

Lewis, James A. “Securing Cyberspace for the 44th Presidency.” Washington, DC: Center for Strategic and International Studies, 2008.

Moon, David B. “Cyber-Herding: Exploiting Islamic Extremists Use of the Internet.” Monterey, CA: Naval Postgraduate School, 1997.

Moran, Daniel. *Wars of National Liberation*. New York: Harper, 2006.

National Science Digital Library. “International Convention for the Suppression of Acts of Nuclear Terrorism (2005).” National Science Foundation. http://www.atomicarchive.com/Treaties/Treaty22.shtml. Accessed March 17, 2009.

Owens, William A., Dam, Kenneth W. and. Lin, Herbert S. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use or Cyber attack Capabilities*. Washington, DC: The National Academies Press, 2009.

Paller, Alan. Paper presented to the United States Senate Committee on Homeland Security and Government Affairs, Washington, DC, April 28, 2009.

Papyrus: Digital Institutional Repository. “Defining the Crime of Aggression: Cutting the Gordian Knot?” Universite de Montreal. https://papyrus.bib.umontreal.ca/jspui/handle/1866/2354. Accessed March 20, 2009.

Privacy International. “U.N. – Convention for the Suppression of Unlawful Seizure of Aircraft (1970).” Privacy International. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-146570. Accessed March 11, 2009.

———. “U.N. – International Convention Against the Taking of Hostages (1979).” Privacy International. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-146575. Accessed March 12, 2009.

Reimer, Jordan. “U.S. Cyber Command Preparations Under Way, General Says.” United States Strategic Command. http://www.stratcom.mil/news/article/150/u.s._cyber_command_preparations_under_way_general_says. Accessed April 15, 2010.

Ross, Dickon. “Electronic Pearl Harbor.” *Guardian*. February 20, 2003.

Serabian, John A. “Cyber Threats and the US Economy.” Central Intelligence Agency. https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html. Accessed June 2, 2009.

Shackelford, Scott J. “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law.” *Berkeley Journal of International Law*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375. Accessed June 1, 2009.

Skoudis, Edward. “Information Security Issues in Cyberspace.” In *Cyberpower and National Security*. Eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz Washington, DC: National Defense University, 2009.

Strategy World, “More Scary Monsters,” *Strategy World*. http://www.strategypage.com/htmw/htiw/articles/20090423.aspx. Accessed June 4, 2009.

Tekwani, Shyam. “The Web of Terror.” *Media Asia* 29, no. 3 (2002).

United Nations. “International Court of Justice.” United Nations. http://www.icj-cij.org/court/index.php?p1=1&PHPSESSID=633d3b8ae47f7c208b91b7833aae8ebd. Accessed May 29, 2010.

———. “Secretary-General Kofi Annan Launches Global Strategy Against Terrorism in Madrid.” United Nations. http://www.un.org/News/Press/docs/2005/sg2095.doc.htm. Accessed June 3, 2009.

United Nations Office on Drugs and Crime. “Convention on Offenses and Certain Other Acts Committed On Board Aircraft 1963 (‘Tokyo Convention’).” United Nations. http://www.unodc.org/pdf/crime/terrorism/Commonwealth_Chapter_2.pdf. Accessed March 11, 2009.

United States Air Force. “Air Force Cyber Command Strategic Vision.” Defense Technical Information Center. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060&Location=U2&doc=GetTRDoc.pdf. Accessed May 14, 2010.

Watkin, Kenneth. "Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict." American Society of International Law. http://74.125.155.132/search?q=cache:CSPE4o2JdroJ:www.asil.org/ajil/watkin.pdf+Kenneth+Watkin,+Controlling+the+Use+of+Force:+A+Role+for+Human+Rights+Norms+in+Contemporary+Armed+Conflict,&cd=1&hl=en&ct=clnk&gl=us&client=firefox-a. Accessed March 22, 2009.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press, 2006.

Weimann Gabriel and Von Knop, Katharina. "Applying the Notion of Noise to Countering Online Terrorism." *Studies in Conflict & Terrorism* 31:1(2008).

Wilson, Clay. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." Washington, DC: Congressional Research Service, 2008.

Wingfield, Thomas C. "International Law and Information Operations." In *Cyberpower and National Security*. Eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Washington, DC: National Defense University Press and Potomac Books, Inc., 2009.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California